IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	**Amdur, et al.**	
Serial No.:	**09/614,487**	Art Unit **2134**
Confirm. No.:	**2054**	
Filed:	**July 11, 2000**	Patent Examiner **Jonathan R. Adams**
For:	**Generation and Use of Digital Signatures**	

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In Response to the Office Action dated January 4, 2005 (the "Action") the Applicants submit as follows:

REMARKS

Claims 11-16 remain pending in the Application. For the reasons set out below, reconsideration of the rejections of the claims is respectfully requested.

The Pending Claims Are Not Anticipated or Obvious in View of the Applied Art

Claim 11 was rejected under 35 U.S.C. § 102(b) as being unpatentable over Mitsitaka, Japanese Patent #11-98134-A (referred to as "'134").

Claim 12 was rejected under 35 U.S.C. § 103(a) as being unpatentable over '134.

Claim 13 was rejected under 35 U.S.C. § 103(a) as being unpatentable over '134 in view of Bruce Schneier, "Applied Cryptography" ("Schneier").

Claim 13 was also stated to be rejected under 35 U.S.C. § 103(a) as being unpatentable over '134 in view of Schneier, and in further view of Devine et al., U.S. Patent No. 6,606.708 ("'708").

These rejections are respectfully traversed.

Additional Comment

Although the Action stated that claim 13 was also rejected in view of '134, Schneier, and '708, Applicants have assumed herein that this rejection includes a typographical error, as the discussion following the rejection refers to claim 14 and not claim 13. Thus, Applicants have proceeded on the assumption that the Office intended claim 14 and not claim 13 to be rejected under 35 U.S.C. § 103(a) as being unpatentable over '134 in view of Schneier, and in further view of '708. If this assumption is not correct, Applicants respectfully submit that claim 14 has not been rejected and therefore should be allowed.

In addition, the Action states that claims 15 and 16 "correspond" to claims 12 and 13, with no statement of rejection. As claims 15 and 16 have not been rejected, Applicants respectfully submit that claims 15 and 16 should be allowed.

The Applied References Do Not Disclose or Suggest
the Features and Relationships Recited in Applicants' Claims

Anticipation pursuant to 35 U.S.C. § 102 requires that a single prior art reference contain all the elements of the claimed invention arranged in the manner recited in the claim. *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983).

Anticipation under 35 U.S.C. § 102 requires in a single prior art disclosure, each and every element of the claimed invention arranged in a manner such that the reference would literally infringe the claims at issue if made later in time. *Lewmar Marine, Inc. v. Barient, Inc.*, 822 F.2d 744, 747, 3 USPQ2d 1766, 1768 (Fed. Cir. 1987).

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q. 2d 1949 (Fed. Cir. 1999).

Before a claim may be rejected on the basis of obviousness pursuant to 35 U.S.C. § 103, the Patent Office bears the burden of establishing that all the recited features of the claim are known in the prior art. This is known as *prima facie* obviousness. To establish *prima facie* obviousness, it must be shown that all the elements and relationships recited in the claim are known in the prior art. If the Office does not produce a *prima facie* case, then the Applicants are under no obligation to submit evidence of nonobviousness. MPEP § 2142.

The teaching, suggestion, or motivation to combine the features in prior art references must be clearly and particularly identified in such prior art to support a rejection on the basis of obviousness. It is not sufficient to offer a broad range of sources and make conclusory statements. *In re Dembiczak*, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

Even if all of the features recited in the claim are known in the prior art, it is still not proper to reject a claim on the basis of obviousness unless there is a specific teaching, suggestion, or motivation in the prior art to produce the claimed combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1568, 1 USPQ2d 1593 (Fed. Cir. 1987). *In re Newell*, 891 F.2d 899, 901, 902, 13 USPQ2d 1248, 1250 (Fed. Cir. 1989).

The evidence of record must teach or suggest the recited features. An assertion of basic knowledge and common sense not based on any evidence in the record lacks substantial evidence support. *In re Zurko*, 258 F.3d 1379, 59 USPQ2d 1693 (Fed. Cir. 2001).

Pending Claim 11 Is Not Anticipated By '134

In the Action claim 11 was rejected under 35 U.S.C. § 102(b) as being anticipated by '134. This rejection is respectfully traversed.

In the Action, the Examiner states that the previous obviousness rejection (Office Action dated February 11, 2004) of claim 11 under 103(a) in view of '134 and Schneier has been withdrawn in view of Applicants' arguments, stated by the Examiner to be persuasive. However, the Examiner takes the position in the current Action that claim 11 is anticipated by '134 alone. It is respectfully submitted that the finding that claim 11 is not obvious in view of '134 and Schneier requires a conclusion that claim 11 is not anticipated by '134, alone.

Further, in the Action, the Examiner states with respect to claim 14 that "'134 does not specifically teach the use of multiple servers" and that it further does not teach "for the client to access a second server and for the second server to authenticate the client's cookie," both of which elements are also found in claim 11.

Thus, the Action acknowledges that the '134 reference does not disclose each and every element of the claimed invention arranged in the manner recited in the claims, as is required to sustain the objection. Hence, Applicants' claim 11 patentably distinguishes over the '134 reference. Therefore, it is respectfully submitted that the 35 U.S.C. § 102(b) rejection has been overcome. It follows that claims 12 and 13 which depend from claim 1 are likewise allowable.

Pending Claims 12 and 13 Are Not Obvious Over '134 in view of Schneier

In the Action claims 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over '134, and '134 in view of Schneier, respectively. These rejections are respectfully traversed. Applicants' response to these rejections is based on the Office's referenced interpretation of these references. Thus, any change in the Office's interpretation of '134 and Schneier shall constitute a new ground of rejection.

As referred to above, in the Action the Examiner states that the previous 103(a) rejection of claim 11 in view of '134 and Schneier has been withdrawn. Claims 12 and 13 are dependent on claim 11. It is respectfully submitted that where an independent claim is held not to be obvious in view of a set of references, it follows that the dependent claims must also be non-obvious in view of the set of references. Thus the rejections of claims 12 and 13 are not proper and should be withdrawn as well.

The Pending Claim 14 Is Not Obvious Over
'134 in view of Schneier and '708

With respect to claim 14, Applicants presume that the Action intended claim 14 to be rejected as being obvious in view of '134, Schneier, and Devine et al., U.S. Patent No. 6,606,708 ("'708"). This presumed rejection is respectfully traversed.

In the Action, the Examiner lists alleged aspects of the '134 reference and then refers to the use of a centralized public key database as disclosed in Schneier. The Examiner then considers the "modified" '134 reference in combination with the teaching of the '708 reference as providing the invention of claim 14 of the present application. With respect, it is submitted that there is no prior art teaching, suggestion or motivation cited to combine these cited references as set out by the Examiner. Therefore it would not have been obvious to a person of ordinary skill in the art at the time of invention to combine the references in a manner which corresponds to the features recited in claim 14.

As the Examiner states, the '134 reference does not disclose the use of multiple servers. Hence there is no "set of server computers" as recited in claim 14 of the present application. Importantly, there is also no disclosure in '134 of encryption of a cookie using a public/private key mechanism. Therefore, a person skilled in the art would not be motivated to combine the '134 reference with the Schneier reference concerning a public key database as the '134 reference does not teach the use of public/private key pairs at all. There would be no motivation to adopt the public key database disclosed in Schneier as the '134 reference is concerned only with symmetric key encryption and therefore there is no prior art teaching or suggestion for combining a teaching that is related to asymmetric public key systems.

It is further submitted that the approach of claim 14 in the present application relates to receipt by a server of an encrypted message (the cookie) from a third party sender (the client computer) where neither the server recipient nor the third party sender carried out the original encryption of the message. Neither the '134 reference nor the Schneier reference describes or suggests such a situation. The approach of the present application is for the encrypting server to include a unique identifier with the encrypted message itself (the cookie). This problem of the cookie being received from a third entity (the client computer) is not described or suggested in the cited art and is not suggested in the references. It is therefore submitted that there is no motivation to combine the '134 and Schneier references and that, even if such a combination did occur, the step of the encrypting server including a unique server identifier in the cookie would not be obvious to one skilled in the art.

The same reasoning applies to the further reference cited by the Examiner, the '708 reference. This reference does not relate to a system in which cookies are encrypted. The reference does not disclose either encryption using a symmetric encryption system or a public key mechanism. There is therefore no prior art teaching, suggestions, or motivation for combining this reference with '134 or Schneier, which deal with encryption of cookies and public key encryption, respectively. Also, the '708 reference does not teach how to accomplish encryption of cookies in an environment with multiple servers.

Even if one skilled in the art were motivated to combine the cited references, which is not admitted, the teachings of the three references do not provide the solution of claim 14 in the present application. The combination asserted by the Examiner at best only results in a multiple-server system with encrypted cookies, combined with a public key database. However, this is

not equivalent to what is claimed in claim 14 of the present application, as that claim 14 recites a set of unique server identifiers that are both used to index the public key database and are available for inclusion in the cookies that are provided to the clients in the system. This solution to the problem of how to decrypt a cookie at a second server when the cookie has been encrypted at a first server computer is not suggested nor made obvious by the teachings of the three cited references.

In addition, there is no teaching or suggestion in the cited references of the retention of the private keys for the encrypted cookies in dynamic memory of the servers. This is a security-enhancing aspect of claim 14 that is not taught or suggested in the cited references. If the private key for the encrypted cookies is not maintained solely in dynamic memory on the first server computer, the security of the encrypted cookies may be compromised.

As the above indicates, the method of claim 14 provides advantages in the ability of a sophisticated multi-server system to securely manage cookies, without the requirement of additional processing at the client side of the system. The security of the encrypted cookies is enhanced by maintaining the private key in dynamic memory of a single server, only. The decryption of a cookie is able to be accomplished by a server that receives the cookie, without the receiving server having to have information apart from what is present in the cookie itself. These advantages are not taught in the prior art, nor are there method steps or structure disclosed to allow such advantages to be achieved. There is a lack of prior art motivation to combine the three references cited and, even if such a combination should be made, the resulting method is missing steps recited in claim 14, which steps would not have been obvious to a person skilled in the art.

It should also be noted that the public key database in the present application does not store keys by their association with users and/or their cookies, but rather claim 14 recites that the database stores keys in association with the server-identifiers in the system. Such an organizational approach permits the dynamic listing of public keys for a given server and thus seamlessly handles the updating of public/private key pairs for the set of servers in the system. (See also claims 15 and 16.) Because of this seamless updating, it is possible to store private keys only in the secure dynamic memories of the servers. This is an important advantage because, in a case where the dynamic management of the public-private key pairs is not supported, it is necessary to retain the private key in a non-volatile memory with the consequent loss of security. Thus, the approach of the current application permits the secure storage of private keys in dynamic memory, an advantage that flows from the method of dynamic management of the public keys described. Such an advantage is not disclosed or suggested in the '134 reference, the Schneier reference, or the '708 reference.

As nothing in the cited art discloses nor suggests the features and relationships that are specifically recited in the claim, and because there is no prior art teaching, suggestion or motivation cited for combining features of the cited references so as to produce Applicants' invention, it is respectfully submitted that the claim is allowable for these reasons. Therefore, it is respectfully submitted that the 35 U.S.C. § 103(a) rejection should be withdrawn. It follows that the claims which depend from claim 14 are likewise allowable.

Pending Claims 15 and 16 Appear Not Rejected

In the Action, the Examiner merely indicates that claims 15 and 16 correspond to claims 12 and 13. No rejection has been applied against claims 15 and 16. For this reason it is submitted that these claims are not rejected, and Applicants request allowance of these claims.

Additional Claim Fees

Please charge the fee associated with a one month extension of time to respond and any other fee due associated with the prosecution of this Application to Deposit Account No. 10-0637 of Walker & Jocke.

Conclusion

Each of Applicants' pending claims specifically recites features and relationships that are neither disclosed nor suggested in any of the applied art. Furthermore, the applied art is devoid of any such teaching, suggestion, or motivation for combining features of the applied art so as to produce Applicants' invention. Allowance of all of Applicants' pending claims is therefore respectfully requested.

The undersigned will be happy to discuss any aspect of the Application by telephone at the Examiner's convenience.

Respectfully submitted,

Ralph E. Jocke Reg. No. 31,029
231 South Broadway
Medina, Ohio 44256
(330) 722-5143